CLAIMS

1. Method for secure and automated transmission of confidential information, in particular an identification code, to an authenticating organization (3) during a transaction with a user (1) according to which a first part of the confidential information is sent to the authenticating organization over a first network, characterized in that it comprises a stage according to which the user (1) sends the second part of the confidential information, complementary to the first part, to a neutral intermediary (4) over a second network (200) disjointed from the first network, the neutral intermediary (4) then sending to the authenticating organization (3), over a third network (300), the complementary part of the confidential information which it has received.

2. Method according to claim 1, characterized in that the two complementary parts are entered on disjointed terminals.

3. Method according to one of claims 1 and 2, characterized in that the transmission of the first part of the confidential information to the authenticating organization (3) is carried out directly between the user (1) and said organization (3) over the first network.

4. Method according to one of claims 1 and 2, characterized in that the transmission of the first part of the confidential information to the authenticating organization (3) is carried out in the following stages:

- the user (1) sends the first part of the confidential information to a supplier of goods or services (2) over the first network (100);
- the supplier (2) then sends the first part to the organization (3) over a third network (300).

5. Method according to one of claims 1 to 4, characterized in that at least one session identifier, shared between at least two of the parties

(1, 2, 3, 4) to the transaction, allow the authenticating organization (3) to reconstitute automatically the confidential information which the user (1) sends to it.

6. Method according to claim 5, characterized in that each session identifier is generated by at least one of the parties (1, 2, 3, 4) to the transaction.

7. Method according to one of claims 1 to 6, characterized in that coordinates for calling back the user (1) over the second network (200) are sent to the neutral intermediary (4) by the authenticating organization (3) over the third network (300).

8. Method according to one of claims 1 to 6, characterized in that coordinates for calling back the user (1) over the second network (200) are sent to the neutral intermediary (4) by the supplier (2) of goods or services over the third network (300).

9. Method according to one of claims 1 to 8, characterized in that the communication over the first network (100) between the user (1) and the authenticating organization (3) or the supplier of goods or services (2) is transferred automatically to the neutral intermediary (4) for the transaction.

10. Method according to claim 9, characterized in that coordinates for calling back the user (1) over the second network (200) are sent to the neutral intermediary (4) by the user (1) over the first network (100).

11. Method according to one of claims 1 to 10, characterized in that the neutral intermediary (4) contacts the user (1) automatically over the second network (200) to retrieve the second complementary part of the confidential information.

12. Method according to one of claims 1 to 6, characterized in that the user (1) contacts the neutral intermediary (4) over the network (200) to send the second complementary part of the confidential information, associated with a session identifier.

13. Method according to one of claims 1 to 12, characterized in that the third network (300) is a secure point to point network.

14. Method according to one of claims 1 to 13, characterized in that the neutral intermediary (4) requests the user (1) to provide, in addition to the confidential information to be sent to the organization (3), a personal code which allows the user (1) to be identified.

15. Method according to claim 14, characterized in that the personal code is sent, via a secure point to point network, to a second authenticating organization with which the user (1) has previously registered or to which the user (1) is known.

16. Method according to one of claims 14 or 15, characterized in that the personal code is a digital or voice code entered on a connected terminal (12).

17. Method according to one of claims 9 to 16, characterized in that the user (1) is automatically guided by the neutral intermediary (4) through the various stages of the method for sending the second part of the confidential information over the first (100) and/or second (200) network respectively, in a coordinated and optionally synchronized manner.

18. Method according to one of claims 1 to 17, characterized in that the user (1) is automatically guided by the various parties (2,3,4) to the transaction through the various information exchange stages over

the first (100) and/or second (200) networks respectively, in a coordinated and optionally synchronized manner.

19. Method according to one of claims 1 to 18, characterized in that the neutral intermediary (4) and/or the organization (3) store(s) the coordinates of user (1) in an uncoded or reversibly encrypted manner.

20. Method according to one of claims 1 to 19, characterized in that the neutral intermediary (4) and/or the organization (3) store(s) in an uncoded or reversible encrypted manner the second complementary part of the confidential information supplied by the user (1) over the network (200).

21. Method according to one of claims 14 to 20, characterized in that the neutral intermediary (4) and/or the organization (3) store(s) the personal code sent by the user (1) in an uncoded or reversible manner.

22. Method according to one of claims 1 to 21, characterized in that the neutral intermediary (4) and/or the organization (3) establish a transaction log.

23. Method according to claim 22, characterized in that the log established by the neutral intermediary (4) and/or the organization (3) is anonymous.

24. Method according to claim 23, characterized in that the anonymity of the log is ensured by a non-decipherable coding of a combination of the coordinates of the user (1) sent over the second network (200) and of the second part of the confidential information sent by the user (1) to the neutral intermediary (4) over the second network (200).

25. Method according to claims 14 to 24, characterized in that the personal code is stored, optionally in combination with the coordinates of the user on the network (200) by means of an undecipherable coding.

26. Method according to one of claims 22 to 25, characterized in that the neutral intermediary (4) sends an advice linked to the transaction log of the user (1) over the network (300).

27. Method according to one of claims 7 to 26, characterized in that the neutral intermediary (4) contacts the user (1) again after the latter has disconnected from the first network (100), said connection to the first network (100) being re-established once the second part of the confidential information has been sent to the neutral intermediary (4).

28. System for securely transmitting confidential information, in particular an identification code, to an authenticating organization (3) during a transaction, comprising means at the location of a user (1) in a transaction with means at an authenticating organization (3) and/or means (21) at a supplier (2) of goods or services, and means (41) at a neutral intermediary (4), characterized in that the means at the location of user (1) comprise means (11) capable of sending a first part of the confidential information to means (21) at the supplier (2) of goods or services or at the organization (3) over a first network (100), means at the location of the user (1) also comprising means (12) capable of sending the second complementary part of the confidential information to means (42) at the neutral intermediary (4) over the second network (200), the means at the neutral intermediary (4) and/or the means at the supplier (2) further comprising means (23, 43) capable of sending the part of the code which they have received to means (33) at the authenticating organization (3).

29. System according to claim 28, characterized in that the first (100) and second (200) networks are disjointed.

30. System according to claim 29, characterized in that the first (100) and second (200) networks use different communication technologies and protocols.

31. System according to one of claims 28 to 30, characterized in that the entry means (11) on the first network (100) are independent of the entry means (12) on the second network (200).

32. System according to one of claims 28 to 31, characterized in that the authenticating organization (3), the neutral intermediary (4) and/or the supplier (2) of goods or services comprise means capable of generating or managing at least one session identifier for exchanging and/or retrieving information concerning the transaction and allowing the authenticating organization (3) to reconstitute the confidential information sent by the user (1) via the entry means (11,12) over the first and second networks (100, 200).

33. System according to one of claims 28 to 32, characterized in that the neutral intermediary (4) comprises means (42, 44) capable of automatically contacting the entry means (12) of the user (1) over the second network (200) so that the user sends the second part of the confidential code.

34. System according to one of claims 28 to 33, characterized in that the neutral intermediary (4) comprises means capable of generating digital fingerprints or unidirectional encryption.

35. System according to one of claims 28 to 34, characterized in that the supplier of goods or services comprises means capable of transferring the communication over the first network (100) between the means of entry (11) at the location of the user connected to server-forming means (21) at the supplier to server-forming means (41) at the neutral intermediary (4), thus automatically connecting the user (1)

to the neutral intermediary (4) and thus enabling the two parties to interact.

36. System according to one of claims 28 to 35, characterized in that the supplier (2) of goods or services, the authenticating organization (3) and the neutral intermediary (4) comprise means (23,33,43) allowing the transmission of secure point to point data over a third network (300).

37. System according to one of claims 28 to 36, characterized in that the neutral intermediary (4) has means (41, 42, 43, 44) enabling it to coordinate and/or synchronize messages over the networks (100, 200 and 300).

38. Systems according to one of claims 28 to 37, characterized in that the neutral intermediary (4) and/or the authenticating organization (3) comprise(s) means (44) capable of storing information supplied by the user (1) and system utilization statistics.

39. System according to one of claims 28 to 38, characterized in that the neutral intermediary (4) comprises means (42) capable of voice recognition and/or voice synthesis.

40. System according to one of claims 28 to 39, characterized in that the user (1) comprises means (12) capable of automatically contacting the server-forming means (42, 44) of the neutral intermediary (4) over the second network (200) in order to send the second part of the confidential code.

41. System according to one of claims 28 to 40, characterized in that the neutral intermediary (4) comprises means capable of being contacted by the user (1) over the second network (200) to enable the transmission of the second part of the confidential information.

42. System according to one of claims 28 to 41, characterized in that the neutral intermediary (4) and/or the organization (3) comprise(s) means capable of identifying the user in a log using the confidential code sent during the transaction.

43. System according to one of claims 28 to 42, characterized in that from its privileged position, the authenticating organization (3) also comprises the means of the neutral intermediary (4).